PN - JP2001144865 A20010525
PD - 2001-05-25
PR - JP19990320316 19991110
OPD - 1999-11-10
TI - IDENTIFICATION SYSTEM USING PORTABLE TELEPHONE SET
IN - UEHATA MASAKAZU
PA - OTSUKA SHOKAI CO LTD
IC - H04M11/00 ; H04Q7/38 ; H04M1/57

TI - Identification system compares user's portable telephone number identified using caller ID and input password with those stored already
PR - JP19990320316 19991110
PN - JP2001144865 A20010525 DW200270 H04M11/00 007pp
PA - (OTSU-N) OTSUKA SHOKAI KK
IC - H04M1/57 ;H04M11/00 ;H04Q7/38
AB - JP2001144865 NOVELTY - The authenticated user's portable telephone numbers and passwords are stored. On receiving a telephone call, the system identifies the caller and compares the number and user input password with those stored already, to identify the individual.
- USE - Identification system using portable telephone set.
- ADVANTAGE - Identifies individuals reliably without requiring the user to carry IC or magnetic cards.
- DESCRIPTION OF DRAWING(S) - The figure shows a schematic representation of the identification system. (Drawing includes non-English language text).
- (Dwg.1/1)
OPD - 1999-11-10
AN - 2002-646951 [70]

PN - JP2001144865 A20010525
PD - 2001-05-25
AP - JP19990320316 19991110
IN - UEHATA MASAKAZU
PA - OTSUKA SHOKAI CO LTD
TI - IDENTIFICATION SYSTEM USING PORTABLE TELEPHONE SET
AB - PROBLEM TO BE SOLVED: To reliably identify an individual without making a user carry with a matter for identifying such as an IC card, a magnetic card in

particular.

- SOLUTION: This identification system comprises an information storing means for storing a users portable telephone member and password, a telephone receiving means, a caller's number recognizing means for recognizing the caller's number of a speech received by the telephone receiving means, a telephone number collating means for collating the caller's number recognized by the caller's number recognizing means with the user's portable telephone number stored in the information storing means, a password receiving mans for receiving the input of the password, and a password collating means for collating the password inputted from the password inputting means with a password corresponding to the caller's number stored in the information storing means.

- H04M11/00 ;H04Q7/38 ;H04M1/57

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－144865
（P2001－144865A）
(43)公開日　平成13年５月25日(2001.5.25)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｍ　11/00	３０１	Ｈ０４Ｍ　11/00	３０１	５Ｋ０３６
	３０３		３０３	５Ｋ０６７
Ｈ０４Ｑ　7/38		1/57		５Ｋ１０１
Ｈ０４Ｍ　1/57		Ｈ０４Ｂ　7/26	１０９Ｓ	

審査請求　有　　請求項の数４　ＯＬ　（全７頁）

(21)出願番号　特願平11－320316

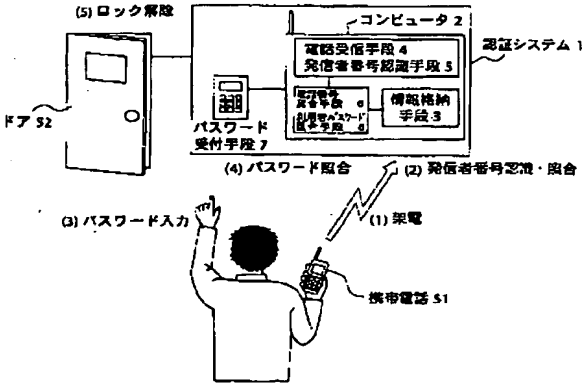
(22)出願日　平成11年11月10日(1999.11.10)

(71)出願人　591281666
株式会社大塚商会
東京都千代田区三崎町２丁目12番１号
(72)発明者　上畑　正和
東京都千代田区三崎町２－12－１　株式会社大塚商会内
(74)代理人　100088214
弁理士　生田　哲郎　（外１名）

Ｆターム(参考)　5K036 AA07 BB18 EE14
5K067 AA21 BB04 BB28 DD17 DD27
EE02 FF07 HH22 HH23 KK15
5K101 LL12 PP03

(54)【発明の名称】　携帯電話を用いた認証システム

(57)【要約】
【課題】利用者がＩＣカードや磁気カード等の認証に用いるための物を特に持ち歩くことなく、確実な本人認証を可能にする。
【解決手段】利用者の携帯電話番号及びパスワードを格納する情報格納手段と、電話受信手段と、該電話受信手段により受信した通話の発信者番号を認識する発信者番号認識手段と、該発信者番号認識手段により認識した発信者番号と前記情報格納手段に格納された利用者の携帯電話番号とを照合する電話番号照合手段と、パスワード入力を受け付けるパスワード受付手段と、該パスワード受付手段から入力されたパスワードと前記情報格納手段に格納されている前記発信者番号に対応するパスワードとを照合するパスワード照合手段とからなることを特徴とする認証システムである。



【特許請求の範囲】
【請求項１】利用者の携帯電話番号を格納する情報格納手段と、電話受信手段と、該電話受信手段により受信した利用者からの架電の発信者番号を認識する発信者番号認識手段と、該発信者番号認識手段により認識した発信者番号と前記情報格納手段に格納された利用者の携帯電話番号とを照合する電話番号照合手段と、からなることを特徴とする認証システム。
【請求項２】利用者の携帯電話番号及び利用者パスワードを格納する情報格納手段と、電話受信手段と、該電話受信手段により受信した利用者からの架電の発信者番号を認識する発信者番号認識手段と、該発信者番号認識手段により認識した発信者番号と前記情報格納手段に格納された利用者の携帯電話番号とを照合する電話番号照合手段と、利用者からの利用者パスワード入力を受け付ける利用者パスワード受付手段と、該利用者パスワード受付手段から利用者により入力されたパスワードと前記情報格納手段に格納されている前記発信者番号に対応する利用者パスワードとを照合する利用者パスワード照合手段と、からなることを特徴とする認証システム。
【請求項３】利用者の携帯電話番号を格納する情報格納手段と、電話受信手段と、該電話受信手段により受信した利用者からの架電の発信者番号を認識する発信者番号認識手段と、該発信者番号認識手段により認識した発信者番号と前記情報格納手段に格納された利用者の携帯電話番号とを照合する電話番号照合手段と、ワンタイム・パスワードを生成するワンタイム・パスワード生成手段と、生成されたワンタイム・パスワードを利用者に対して伝達する伝達手段と、利用者からのワンタイム・パスワード入力を受け付けるワンタイム・パスワード受付手段と、該ワンタイム・パスワード受付手段から利用者により入力されたパスワードと前記生成されたワンタイム・パスワードとの同一性を照合するワンタイム・パスワード照合手段と、からなることを特徴とする認証システム。
【請求項４】利用者の携帯電話番号及び利用者パスワードを格納する情報格納手段と、電話受信手段と、該電話受信手段により受信した利用者からの架電の発信者番号を認識する発信者番号認識手段と、該発信者番号認識手段により認識した発信者番号と前記情報格納手段に格納された利用者の携帯電話番号とを照合する電話番号照合手段と、利用者からの利用者パスワード入力を受け付ける利用者パスワード受付手段と、該利用者パスワード受付手段から利用者により入力されたパスワードと前記情報格納手段に格納されている前記発信者番号に対応する利用者パスワードとを照合する利用者パスワード照合手段と、ワンタイム・パスワードを生成するワンタイム・パスワード生成手段と、生成されたワンタイム・パスワードを利用者に対して伝達する伝達手段と、利用者からのワンタイム・パスワード入力を受け付けるワンタイム・パスワード受付手段と、該ワンタイム・パスワード受付手段から利用者により入力されたパスワードと前記生成されたワンタイム・パスワードとの同一性を照合するワンタイム・パスワード照合手段と、からなることを特徴とする認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、利用者が本人であることを認証するための、認証システムに関するものである。
【０００２】
【従来の技術】あるシステムの利用に際し、当該システムが、これを利用しようとする者の利用権を判断するための認証方法としては、生物学的な特徴を利用する方法、パスワードを利用する方法、認証のための装置を携帯する方法が存する。
【０００３】生物学的な特徴を利用する方法としては、指紋、声紋、網膜、筆跡などを用いる方法があるが、精度の高い認証のためにはシステム構築費用が高額となり、また、生物学的・身体的特徴を利用するという方法には利用者の抵抗感が強いという問題がある。
【０００４】パスワードを利用する方法は広く利用されているが、パスワードが盗まれる可能性は常に存する。この場合のセキュリティホールは３箇所が想定される。すなわち、パスワードファイル等が蓄積されているサーバ、サーバと利用者との通信手段、及び利用者自身である。従来よく利用されている、利用者が自己のパスワードを設定してこれをシステムに登録しておき、システムが、利用者が利用の際に入力したパスワードと登録されているパスワードを照合する方式の場合、利用者は自分自身もパスワードを記憶しておく必要があるため、誕生日等の自己に何らかの関係を有するパスワードを選択することが多く、これを手がかりとしてパスワードが盗用される危険が大きい。また、サーバや通信手段に対するハッキングの危険も高い。
【０００５】そこで、通常のパスワードよりも安全な方法として、ワンタイム・パスワードという方式が考案されている。ワンタイム・パスワードは、使い捨てパスワード、ダイナミック・パスワード等とも呼ばれ、１回限り使用されるパスワードである。
【０００６】すなわち、利用者は、認証サーバと同期するトークン発生器を所持しており、トークン発生器は一定時間ごとに認証サーバと同期してパスワードを生成する。利用者は、開錠する際に当該トークン発生器に表示されたパスワードを入力する。認証サーバは、パスワードの入力があったときの時刻におけるパスワードを生成し、入力されたパスワードと照合を行う。すなわち、このときトークン発生器によって生成されるパスワードは一定時間の間しか使用することができず、しかも、用いられるとその後は使用できなくなる。パスワードが時々

刻々と変化する点で、極めて安全性が高い。なお、以上説明した方式は、ワンタイム・パスワードのうちの時間同期方式と呼ばれるものであるが、ワンタイム・パスワードには、他に、非同期方式、カウンタ同期方式が存する。

【０００７】しかし、この方式の場合には、トークン発生器を利用者が所持する必要があり、結局次に述べる方法である認証のための装置を携帯する方法の欠点を有することとなる。

【０００８】次に、認証に用いる装置等を携帯する方法とは、利用者が、ＩＣカードや、前記のトークン発生器等を携帯する方法である。この方法の欠点としては、認証のためだけに特定の装置等（ＩＣカード等）を持ち歩くのが利用者にとって煩雑であること、コストが高くなることなどがあげられる。認証のために用いる装置等は、大きければ持ち歩くのに不便であり、しかし、利用者が持ち歩きやすいように小型化すれば紛失の危険が増大する。

【０００９】

【発明が解決しようとする課題】以上述べたように、それぞれの方式にはメリットもあるが、それぞれ問題点もあり、セキュリティを高めようとすると、コストが高くなり、あるいは利用者に負担をかけることとなっていた。本発明は、このような従来の問題点を解決すべく、安全性が高く、かつシステムとして安価で、しかも利用者にとって負担の少ない認証システムを提供することを課題としている。

【００１０】

【課題を解決するための手段】この課題を解決するため、請求項１の発明は、利用者の携帯電話番号を格納する情報格納手段と、電話受信手段と、該電話受信手段により受信した利用者からの架電の発信者番号を認識する発信者番号認識手段と、該発信者番号認識手段により認識した発信者番号と前記情報格納手段に格納された利用者の携帯電話番号とを照合する電話番号照合手段と、からなることを特徴とする認証システムである。

【００１１】本発明の認証システムは、携帯電話の発信者番号を利用して認証をおこなう。架電があった場合に、当該架電の発信者番号を認識する機能は公知であり、すでに利用されている。このとき、携帯電話本体に埋め込まれた電話番号情報は高度なセキュリティ機能により防衛されているので第三者が不正に改変することが困難である。本発明は、このような、携帯電話が有するセキュリティ機能を利用する。すなわち、本発明の認証システムは、利用者による携帯電話からの架電を受信することにより認識された発信者番号を、事前に登録された利用者の携帯電話番号と照合することで、当該電話通信が、確かに登録された利用者の携帯電話から発せられたものであることを確認する。したがって、このシステムによれば、現在システムを使用しようとしている者が、少なくとも登録された携帯電話を所持する者であることが保証される。

【００１２】このシステムを用いれば、利用者は、ＩＣカードや磁気カード等の、認証に用いるための物を特に持ち歩く煩わしさがなく、ただ自分が普段利用している携帯電話の番号を登録しておくだけで、システムに対し本人であることを示すことが可能になる。また、携帯電話を紛失した場合においても、単なるＩＣカード等を紛失した場合と比べて紛失の事態を早期に発見しやすいと解され、その意味でも高いセキュリティを確保しうる。

【００１３】システムを提供する側にとっても、ＩＣカード等を特に用意する必要がなく、安価に、しかも確実に認証を行うことができるという大きな利益がある。さらに、認証を試みた者の発信者番号等のログを残すことができるため、高いセキュリティ管理を行いうる。

【００１４】なお、この発明及び以下の発明にいう携帯電話とは、ＰＤＳ、ＰＨＳ等の一般に普及している公衆通話に用いられるものに限られず、ポケットベルやその他、例えば特定の施設内での連絡用に使用されている通話装置など移動体通信装置全般を含む。

【００１５】請求項２記載の発明は、利用者の携帯電話番号及び利用者パスワードを格納する情報格納手段と、電話受信手段と、該電話受信手段により受信した利用者からの架電の発信者番号を認識する発信者番号認識手段と、該発信者番号認識手段により認識した発信者番号と前記情報格納手段に格納された利用者の携帯電話番号とを照合する電話番号照合手段と、利用者からの利用者パスワード入力を受け付ける利用者パスワード受付手段と、該利用者パスワード受付手段から利用者により入力されたパスワードと前記情報格納手段に格納されている前記発信者番号に対応する利用者パスワードとを照合する利用者パスワード照合手段と、からなることを特徴とする認証システムである。

【００１６】これは、携帯電話が盗難された場合に「なりすまし」が可能となってしまうという問題点に対処するため、さらに、パスワードによる認証を付加した、請求項１記載の認証システムである　発信者番号と利用者パスワードとで二重の認証を行うことで、さらに高い安全性が確保される。ここでいう利用者パスワードとは、利用者あるいはシステム設定者等があらかじめ決定して、照合のためにシステムに記憶しておくタイプの、一般によく使用されるパスワードである。利用者は、本発明の認証システムに携帯電話で架電することにより、当該携帯電話の所持者であることの認証を受けたうえで、利用者パスワードを入力することにより、二重の認証を受ける。

【００１７】なお、利用者パスワード受付手段は、携帯電話からの架電を介し携帯電話のプッシュボタンからの入力を受け付けるものであってもよいし、システムにハードウェアとしてテンキー等の入力手段を用意してもよ

い。

【００１８】請求項３記載の発明は、利用者の携帯電話番号を格納する情報格納手段と、電話受信手段と、該電話受信手段により受信した利用者からの架電の発信者番号を認識する発信者番号認識手段と、該発信者番号認識手段により認識した発信者番号と前記情報格納手段に格納された利用者の携帯電話番号とを照合する電話番号照合手段と、ワンタイム・パスワードを生成するワンタイム・パスワード生成手段と、生成されたワンタイム・パスワードを利用者に対して伝達する伝達手段と、利用者からのワンタイム・パスワード入力を受け付けるワンタイム・パスワード受付手段と、該ワンタイム・パスワード受付手段から利用者により入力されたパスワードと前記生成されたワンタイム・パスワードとの同一性を照合するワンタイム・パスワード照合手段と、からなることを特徴とする認証システムである。

【００１９】これは、パスワードとして、通常のパスワードシステムより安全性の高いワンタイム・パスワードを用い、発信者番号の照合と共に用いることで安全性を高めた、請求項１記載の認証システムである。

【００２０】本発明の装置は、ワンタイム・パスワードを用いた認証システムであるが、携帯電話を使用してシステムからワンタイム・パスワードを取得することで、いわば、携帯電話をトークン発生器等の代わりに用いるものである。これにより、従来のワンタイム・パスワードを用いるシステムが有していた、トークン発生器等のハードウェアをわざわざ携帯することが利用者にとって煩わしいという欠点、及び複雑なトークン発生器を要することによりシステムが高価となるという欠点が回避できる。

【００２１】従来のワンタイム・パスワードを用いる認証システムは、トークン発生器自身がシステム本体と同じアルゴリズムを用いてワンタイム・パスワードを生成するものである。これに対し、本発明の認証システムでは、ワンタイム・パスワードの生成はシステム本体のワンタイム・パスワード生成手段により行い、利用者はこれを携帯電話等を介して受け取る点が異なる。ワンタイム・パスワードを利用者に対して伝達する伝達手段は、基本的には携帯電話を介するものであるが、携帯電話を介しないものでもよく、また、ディスプレイ等に表示するものばかりでなく、音声等によって利用者に伝達する手段も含まれる。ワンタイム・パスワード生成手段は、一定時間間隔を有する時刻毎に、その時刻におけるパスワードを生成する。

【００２２】ワンタイム・パスワード照合手段は、システムから要求されて利用者がワンタイム・パスワードを入力した時点で、ワンタイム・パスワード生成手段によってその時刻（及び、それ以前の一定の時刻）におけるワンタイム・パスワードを再度生成して、これを利用者により入力されたパスワードと照合するという方法を採用することも可能であるし、利用者に対して伝達したワンタイム・パスワードをシステムが保持し、一定時間内に利用者が当該ワンタイム・パスワードを入力した場合にのみ本人と認証するという方法を採用することも可能である。後者の方法は、本発明の認証システムにおいては、トークン発生器によりワンタイム・パスワードの生成を行うのではなく、システム本体が行うことから可能となる。また、本発明にいうワンタイム・パスワードには、利用者により入力される文字列そのもののみならず、それを生成するためのキーとなるコードを含む。たとえば、利用者が、システムから伝達されたコードに何らかの操作を加えたうえでシステムに文字列等を入力する場合、その元になるコードもワンタイム・パスワードに含まれ、かつ当該コードに利用者が操作を加えた文字列等と、当該コードにシステムが同様の操作を加えて作成した文字列を比較する場合等も、本発明でいうところの、ワンタイム・パスワードの照合である。その他、公知のワンタイム・パスワードによる認証システムにおける照合方法は、すべて本発明におけるワンタイム・パスワード照合手段に含まれる。

【００２３】請求項４記載の発明は、利用者の携帯電話番号及び利用者パスワードを格納する情報格納手段と、電話受信手段と、該電話受信手段により受信した利用者からの架電の発信者番号を認識する発信者番号認識手段と、該発信者番号認識手段により認識した発信者番号と前記情報格納手段に格納された利用者の携帯電話番号とを照合する電話番号照合手段と、利用者からの利用者パスワード入力を受け付ける利用者パスワード受付手段と、該利用者パスワード受付手段から利用者により入力されたパスワードと前記情報格納手段に格納されている前記発信者番号に対応する利用者パスワードとを照合する利用者パスワード照合手段と、ワンタイム・パスワードを生成するワンタイム・パスワード生成手段と、生成されたワンタイム・パスワードを利用者に対して伝達する伝達手段と、利用者からのワンタイム・パスワード入力を受け付けるワンタイム・パスワード受付手段と、該ワンタイム・パスワード受付手段から利用者により入力されたパスワードと前記生成されたワンタイム・パスワードとの同一性を照合するワンタイム・パスワード照合手段と、からなることを特徴とする認証システムである。

【００２４】これは、発信者番号の他に、利用者パスワード及びワンタイム・パスワードを要求して三重のセキュリティをかけることにより、極めて高い安全性を確保したことを特徴とする認証システムである。請求項１ないし請求項３における説明は、この発明にも該当する。利用者は、本発明の認証システムに携帯電話で架電することにより、まず当該携帯電話の所持者であることで認証を受け、さらに利用者パスワードとワンタイム・パスワードによる認証を受ける。

【００２５】
【発明の実施の形態】
【実施例１】電子的に施錠されたドアに接続され、登録された利用者による施錠解除要求の場合にのみ当該ドアの施錠を解除するシステムにおける本発明の認証システムの使用例を図１に基づき説明する。
【００２６】認証システム１は、電話受信手段４及び発信者番号認識手段５を有するコンピュータ２において実現され、情報格納手段３、発信者番号と利用者の携帯電話番号を照合する電話番号照合手段６、利用者パスワード照合手段８はコンピュータ２においてソフトウェアを用いて実現される。さらに、コンピュータ２には入力パッドである利用者パスワード受付手段７が接続されている。
【００２７】利用者はまず、本件認証システムに事前に番号を登録してある携帯電話５１から、本件認証システム１に対し電話をかける（図１（１））。本件認証システム１は、電話受信手段４により利用者からの電話を受信して、発信者番号認識手段５により発信者番号を認識し、当該発信者番号が、あらかじめ情報格納手段３に登録されているものであるか否かを電話番号照合手段６により照合する（図１（２））。
【００２８】この照合の結果、電話をかけてきた利用者の発信者番号が登録されたものであることが確認されると、次に、本件認証システム１は、ドアの脇に設けられたディスプレイによって利用者に対し、利用者パスワードの入力を促す。
【００２９】これに応じて利用者が利用者パスワード受付手段７からパスワードを入力すると（図１（３））、本件認証システム１は受け取ったパスワードと、情報格納手段３に登録されているパスワードのうち前記確認した発信者番号に対応するパスワードとの照合を利用者パスワード照合手段８により行う（図１（４））。その結果、登録された利用者パスワードと、利用者により入力されたパスワードが一致することが確認されると、本件認証システム１は、ドア５２の施錠を解除する旨の指令を出して、施錠を解除する（図１（５））。
【００３０】施錠は一定の間解除され、一定時間が経過するか、あるいはドア５２が一度開閉すると再び施錠される。
【００３１】
【実施例２】次に、本発明をモバイル携帯端末によるリモート・ログイン・システムに使用する例として、サーバコンピュータ（以下、「本件サーバ」という。）に本発明の認証システムが組み込まれ、利用者によるモバイル端末によるリモート・ログインを受け付ける例を図２に基づき説明する。
【００３２】認証システムは、電話受信手段及び発信者番認識手段を有するコンピュータ（ＲＡＳサーバ）において構成され、情報格納手段、電話号照合手段、利用者パスワード受付手段、利用者パスワード照合手段、ワンタイム・パスワード生成手段、ワンタイムパスワード伝達手段、ワンタイム・パスワード受付手段、ワンタイム・パスワード照合手段が、通信手段を有する当該コンピュータにおいてソフトウェアを用いて実現されている。これらはここでは図示しない。情報格納手段（記憶装置）には、利用者のログイン名、携帯電話番号及び利用者パスワード等の情報が記憶されている。
【００３３】利用者は、モバイル携帯端末により外部から本件サーバにログインしようとするとき、まず、自己の携帯電話５１から認証システム１に電話をかける（図２（１））。認証システム１はこの電話を受けると、発信者番号認識手段により利用者の発信者番号を認識する（図２（２））。そして電話番号照合手段により、当該発信者番号を、情報格納手段に記憶している利用者の携帯電話番号と順次照合する（図２（３））。そして、一致するものがあった場合に、この携帯電話番号の所持者がログインを希望しているものと想定し、さらに当該携帯電話の所持者が本人（当該携帯電話番号に対応するログイン名を有する本人）であることを確認するために、当該架電を通じて利用者に対し、利用者パスワードを要求する（図２（４））。
【００３４】これに応じて利用者が、当該架電を通じて携帯電話のプッシュダイヤルを押すことによりパスワードを入力すると、認証システム１は利用者パスワード受付手段によりこれを受け取り（図２（５））、前記ログイン名に対応する記憶された利用者パスワードと、入力されたパスワードを利用者パスワード照合手段により照合する（図２（６））。これが一致すると、次に認証システム１は、ワンタイム・パスワード生成手段によりその時刻におけるワンタイム・パスワードを生成し、ワンタイム・パスワード伝達手段により当該架電を通して利用者に対し送信する（図２（７））。利用者はこのワンタイム・パスワードを記憶しておく。
【００３５】以後の手順は、利用者側のモバイル端末５３と、認証システム１との間で通信を介して行われる。利用者は、前記記憶したワンタイム・パスワードが有効である一定時間内に、本件認証システム１にログインを要求する（図２（８））。これは、インターネットのプロバイダーを介してもよい。
【００３６】利用者がログイン名を入力してログインを要求すると、本件認証システム１は、利用者に対し、ワンタイム・パスワードの入力を要求する（図２（９））。これに応じて利用者が、前記記憶したワンタイム・パスワードをワンタイム・パスワード受付手段に対し入力すると（図２（１０））、認証システム１は、その時刻においてワンタイム・パスワードを生成し、その時刻におけるワンタイム・パスワード（及び、それ以前の数回分のワンタイム・パスワード）と、入力されたパスワードをワンタイム・パスワード照合手段により照

合する（図2（11））。そして、これが一致した場合に、当該利用者のログインを承認する（図2（12））。以上のように、本件認証システム1は、図2（2）（3）（4）（6）（7）（9）（11）（12）の手順をソフトウェアを用いて実行する。

【0037】

【発明の効果】以上のように、本発明の認証システムは、利用者が特別なカードやハードウェアを所持することなく、高度なセキュリティを実現することができる。

【図面の簡単な説明】

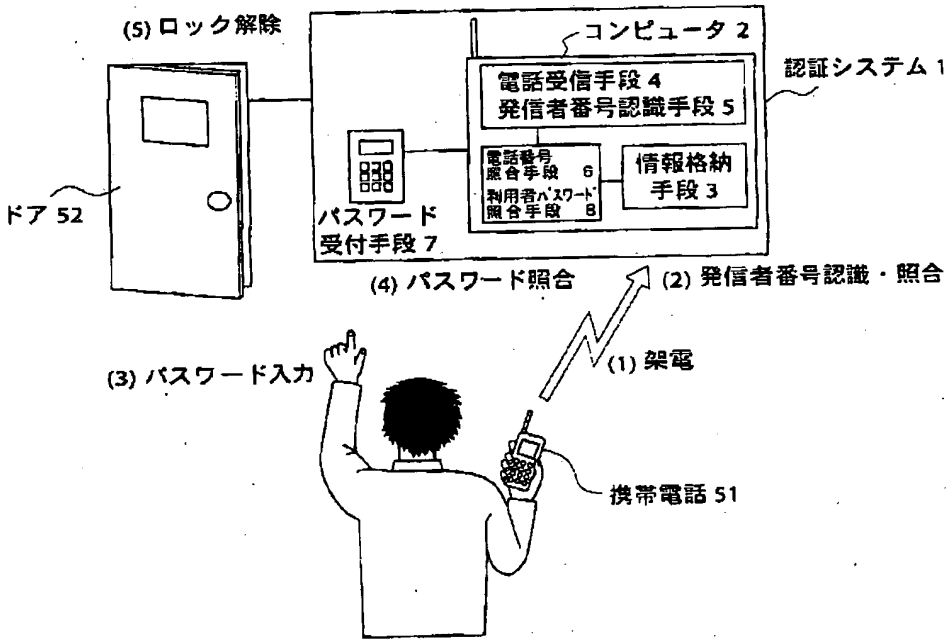
【図1】　本発明の自動ドアシステムにおける実施例

【図2】　本発明のリモート・ログイン・システムにおける実施例

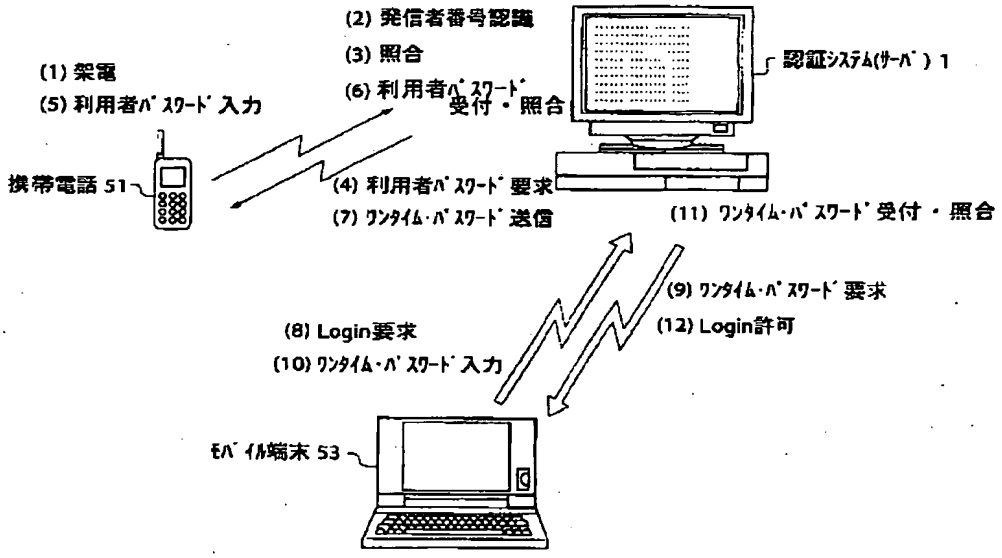
【符号の説明】

1	認証システム
2	コンピュータ
3	情報格納手段
4	電話受信手段
5	発信者番号認識手段
6	照合手段
7	パスワード受付手段
8	照合手段
51	携帯電話
52	ドア
53	モバイル端末

【図1】



【図2】


(2) 発信者番号認識
(3) 照合
(1) 架電
(5) 利用者ﾊﾟｽﾜｰﾄﾞ入力
(6) 利用者ﾊﾟｽﾜｰﾄﾞ
受付・照合
認証ｼｽﾃﾑ(ｻｰﾊﾞ) 1
携帯電話 51
(4) 利用者ﾊﾟｽﾜｰﾄﾞ要求
(7) ﾜﾝﾀｲﾑ･ﾊﾟｽﾜｰﾄﾞ送信
(11) ﾜﾝﾀｲﾑ･ﾊﾟｽﾜｰﾄﾞ受付・照合
(9) ﾜﾝﾀｲﾑ･ﾊﾟｽﾜｰﾄﾞ要求
(12) Login許可
(8) Login要求
(10) ﾜﾝﾀｲﾑ･ﾊﾟｽﾜｰﾄﾞ入力
ﾓﾊﾞｲﾙ端末 53